Healthcare Company takes proactive measures to improve security maturity

Case Study

- **Industry:** Healthcare
- **Country:** United States
- **Size:** Mid-size

Challenges

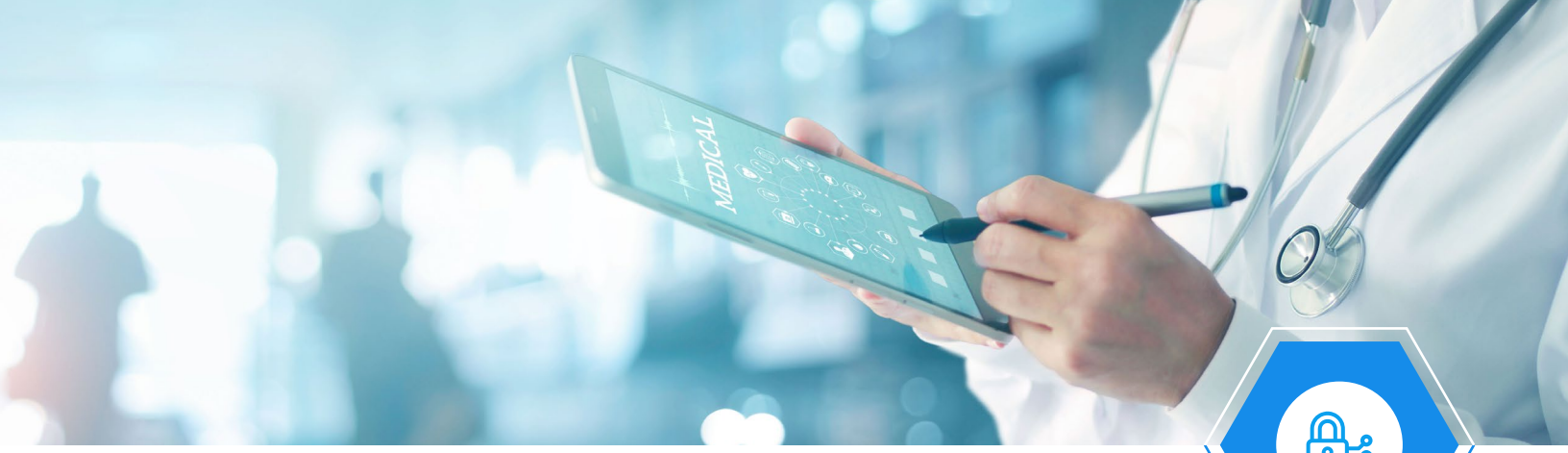
- A compromise revealed security gaps.
- Limited organizational support to increase security budget.
- Lacked automated tools to assist small IT and security teams.

Solutions

- The Arete Cyber Strategy and Defense team conducted a complete risk assessment.
- Ongoing virtual CISO (vCISO) collaboration for best-practice guidance regarding technology and documentation on standard operating procedures and controls.

Benefits

- Gained baseline of current cyber hygiene.
- Achieved executive and board support to add a new budget for security tools and recurring assessments.
- Developed a new plan to harden existing infrastructure and take security maturity to the next level.



Having experienced an eye-opening compromise on an outdated platform, a growing healthcare company opted to take its incident response (IR) investigation to the next level, engaging the Arete Cyber Strategy and Defense team to perform a complete risk assessment.

The company's chief information officer (CIO) saw the incident as an opportunity not only to measure and get a baseline of its cyber hygiene, but also devise a plan for hardening its infrastructure and reaching a higher level of security maturity.

Hitting the reset button on security

"In the past, we'd conducted a pen-test and an annual internal assessment. We knew we needed to do more but didn't have the necessary organizational support to perform more recurring procedures," the CIO said. "The compromise was a reset moment that initiated more focus and investment in security."

"We expected a less than perfect score, especially as this was our first external assessment, but it was invaluable to have the Arete team available to provide context for our CEO and board members."

The Arete Cyber Strategy and Defense team ran a thorough assessment of 170 administrative, technical, and process controls to identify risks and threats. The findings weren't a complete surprise — they did, indeed, reveal some weaknesses and areas for improvement.

"We didn't know what we didn't know," the CIO said. "We expected a less than perfect score, especially as this was our first external assessment, but it was invaluable to have the Arete team available to provide context for our CEO and board members. They explained that while our score wasn't an A+, it was higher than average and gave us a good baseline from which to grow and improve."

Findings and recommendations

Per the assessment, the company got docked points for lacking certain technology and written documentation and policies around standard operating procedures and controls. For example, it had neither a system to manage privileged access management accounts nor one to collect logs. Moreover, many tasks were performed manually — not ideal for a small IT staff and an even smaller security staff that has multiple roles to play.

To kickstart progress, the Arete Cyber Strategy and Defense team provided strategic and technical recommendations for the long-term development and improvement of the company's security posture. What's more, they helped the internal IT team build a strong case to present to executive leadership to gain support in securing additional budget.

"Prior to the assessment, leadership had other priorities," the CIO said. "Arete helped pinpoint areas where we could begin to make improvements and maximize resources. Their insights convinced the CEO to add the necessary budget to procure new technology, including a privileged account management platform. On its own, the platform will significantly raise our overall security maturity rating."

By automating local domain admin account provisioning, not only will the platform help reduce the burden on the IT and security teams, but from a cybersecurity perspective and in the case of another compromise, it will also help minimize any lateral attacks by segmenting everything.

"Arete helped pinpoint areas where we could begin to make improvements and maximize resources. Their insights convinced the CEO to add the necessary budget to procure new technology, including a privileged account management platform."

Ongoing partnership and collaboration

Currently, the company's IT team is in the process of reformatting 100 policy and standard operating procedure documents and has identified Arete for potential staff augmentation. Should they face a time crunch in creating certain documents and policies, they know they can always reach out to the Cyber Strategy and Defense team for additional support.

"No matter how busy the Arete team is, they always make time for us when we need them," the CIO said. "They are easy to reach and fast to respond with thorough, detailed answers to our questions."

As part of the engagement, the Arete Cyber Strategy and Defense team is also providing security and architectural oversight of the development of the company's new website; and the CIO continues to meet weekly with an Arete virtual CISO (vCISO) to collaborate on further development and execution of the company's new information security plan.

"My weekly meetings with the vCISO are an ongoing validation of our project execution," the CIO said. "I update him on the various activities my team is currently engaged on, and he's available to help where needed — from proofreading a policy document to providing best-practice recommendations to hopping on a call with the executive team to offer an external perspective. He's especially skilled at helping everyone understand the nuanced complexities of certain challenges."

Getting ahead of threats

While the company had previously deployed the SentinelOne endpoint detection and response (EDR) platform to its 3,000 endpoints, including servers, it is now working with Arete's in-house SentinelOne consultant to implement best practices that will further raise its security rating. At the same time, the company is looking to deploy a security information and event monitoring (SIEM) system for log collection to help ensure forensic visibility in the case of any future security events.

"Working with Arete's team of strategy and defense specialists has been a very positive experience," the CIO said. "They appreciate that we are proactive, open to suggestions, and want to face and not hide our challenges. Together, we're working to get as far ahead of threats as possible."

"Working with Arete's team of strategy and defense specialists has been a very positive experience."

Arete transforms the way organizations of all sizes and across all industries prepare for and respond to cyberattacks. With decades of experience fighting cybercrime, our global team of cybersecurity experts has been on the front lines of some of the world's most challenging data breaches and ransomware attacks. Arete's complete offerings — incident response, digital forensics, restoration, managed detection and response, endpoint protection, threat intelligence, threat hunting, and advisory and consulting services — help our clients address the full threat life cycle while also strengthening their overall cyber posture. To learn more, visit www.areteir.com or follow us @Arete_Advisors.

Arete